**Simetrik Şifreleme Mesajlaşma Uygulaması Dökümantasyonu**

**Ahmet Hakan TULGAÇ**

## **İÇİNDEKİLER**

1. Giriş................................................................................................................................................ 3

2 Amaç ............................................................................................................................................... 3

3 Kapsam ............................................................................................................................................4

4 Uyguluma........................................................................................................................................4

4.1 Akış Diyagramı ......................................................................................................................... 5

4.2 Sözde Kod ............................................................................................................................... 6

4.3 Uygulama Görüntüleri ............................................................................................................. 7

4.3.1 Giriş Ekranı....................................................................................................................... 7

4.3.2 Sohbet Odası Giriş Ekranı................................................................................................. 8

4.3.3 Sohbet Ekranı................................................................................................................... 9

4.3.4 Mesajların Veritabanında Tutulması............................................................................... 10

5 İlgili Çalışmalar..................................................................................................................................11

6 Sonuç................................................................................................................................................12

7 Kaynakça...........................................................................................................................................13

**1.Giriş**

Android işletim sistemi için geliştirilen bu uygulama, bir kullanıcın oluş- turduğu sohbet odasının numarasını bilen diğer kullanıcıların, bu odaya dahil olarak sohbet etmelerini sağlar. Yazılan mesajlar veri tabanına kaydedilirken bir şifreleme algoritması kullanılır. Mesaj kaydedildikten sonra sayfa anlık olarak güncellenir ve yeni eklenen mesajın veri tabanındaki şifreli hali, şifreleme algo- ritmasının simetriği kullanılarak güncel mesajlar kısmına eklenir.

**2.Amaç**

Kullanıcıların, güncel bir sohbet odasında yazdıkları mesajların, sadece o oda numarasını bilen kullanıcılar tarafından görüntülenmesi gerekir. Yazılan mesajlar, veri tabanında şifreli bir şekilde tutulmalı ve bu mesajlar sohbet odasında tekrardan yazdırılırken, eksiksiz ve hatasız olmalıdır.

**3.Kapsam**

Uygulamanın kapsadığı kullanıcı tipleri aşağıdaki gibidir;

3.1.Mesaj Yazan Kullanıcı

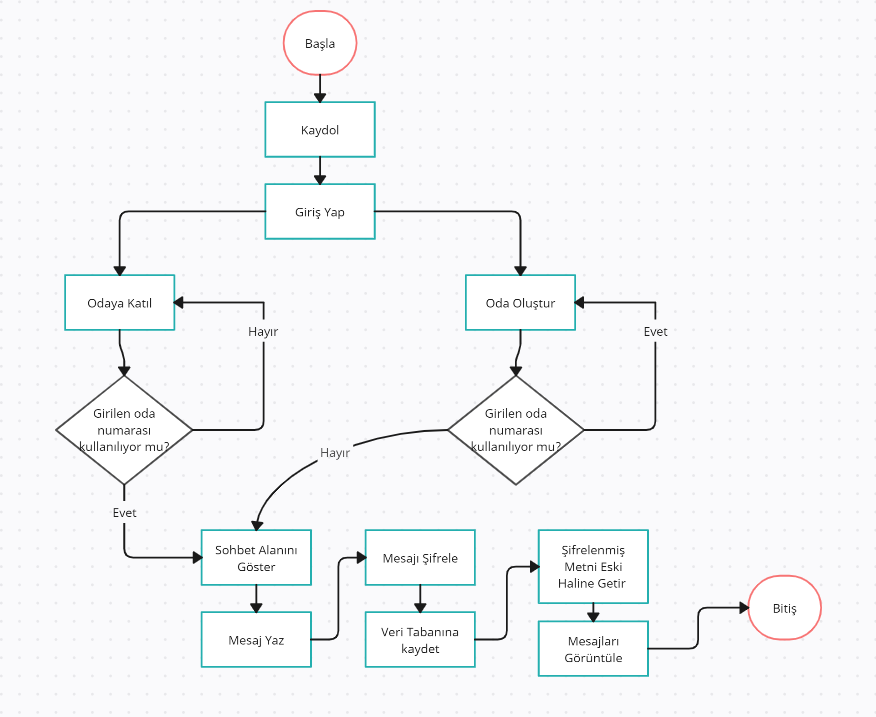
* Oda oluşturur ya da var olan odaya katılır.
* Yazdığı mesaj veri tabanına kaydedilir ve mesaj aynı şekilde sohbet kısmında görüntülenir.
* Yazdığı mesajlar sağa dayalı bir şekilde görüntülenir.

3.2.Mesajları Görüntüleyen Kullanıcılar

* Var olan bir odanın numarası ile odaya dahil olurlar.
* Bulundukları odada kendilerinin mesajları da dahil olmak üzere, önceden yazılmış tüm mesajları görüntülerler.
* Yazılan mesajlar sola dayalı bir şekilde görüntülenir.
* Tüm mesajlar veri tabanında şifreli bir şekilde tutulmalıdır.

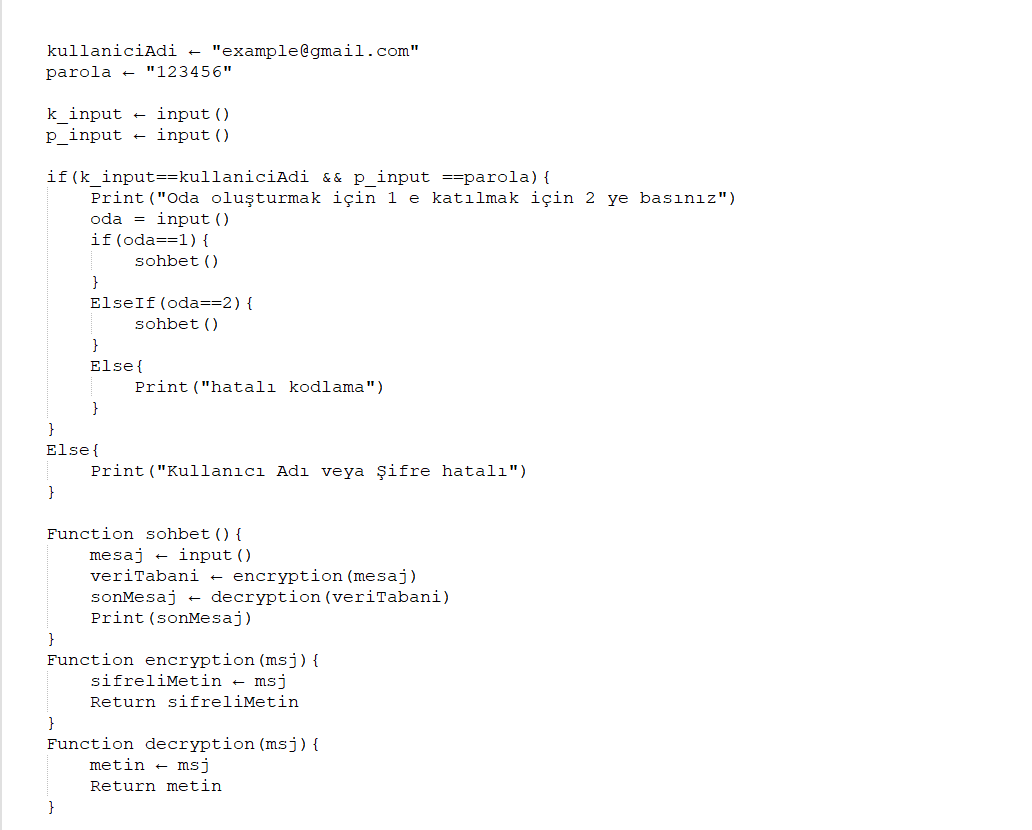
**4.Uygulama**

**4.1.Akış diyagramı**

****

***Şekil4.1.1***

**4.2.Sözde Kodu**

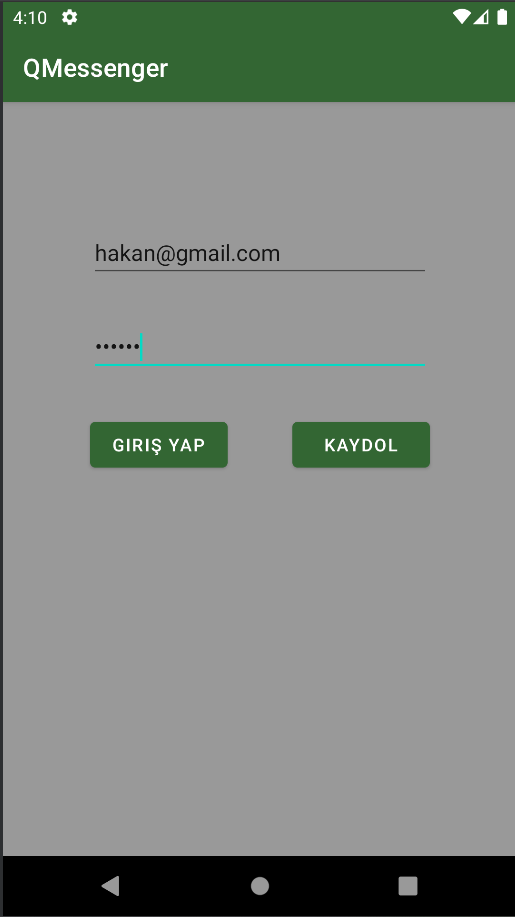
****

***Şekil 4.2.1***

**4.3.Uygulama Görüntüleri**

**4.3.1.Giriş Ekranı**

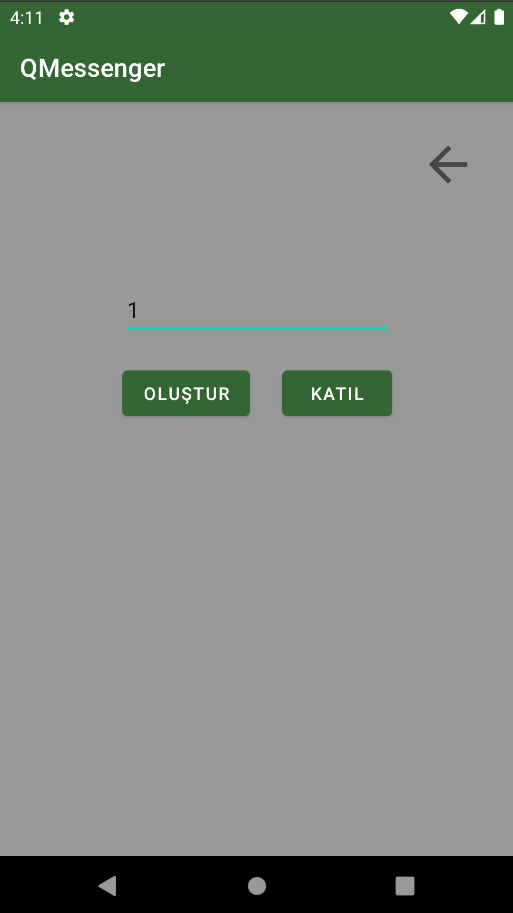
Email ve parola kısımları doldurulur, eğer girilen bilgiler, kayıtlarda olan kullanıcılardan birine ait değilse kaydol butonuna dokunulması halinde yeni kullanıcı kaydedilir, kayıtlı kullanıcı ise giriş yap butonuna basılması halinde kullanıcı girişi yapılır.



***Şekil 4.3.1.1***

**4.3.2.Sohbet Odası Girişi Ekranı**

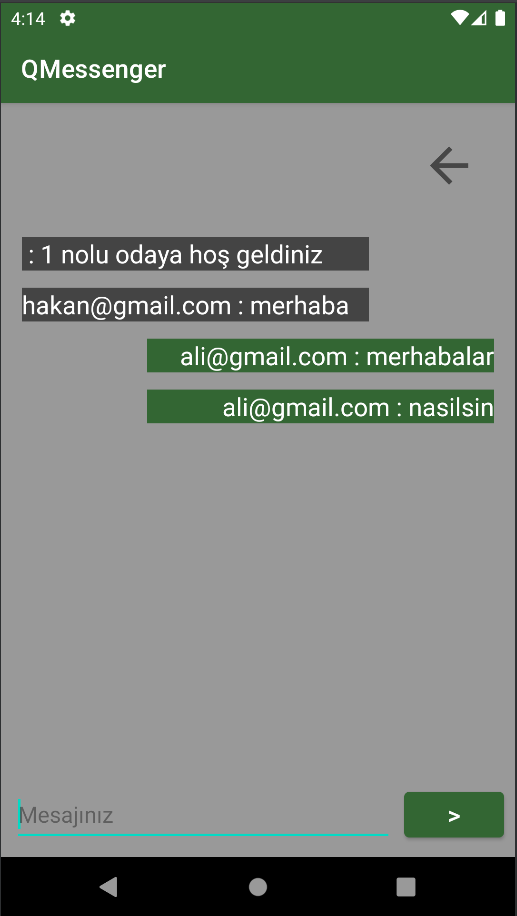
Bir sohbet odası numarası girilir. Girilen numara daha önceden oluşturulan bir odanın numarasıysa, katıl butonuna dokunulduğunda, bu odaya katılım sağlanır. Oda numarası, önceden oluşturulmamışsa, oda o- luştur butonuna dokunulduğunda yeni oda oluşturulur.



***Şekil 4.3.2.1***

**4.3.3.Sohbet Ekranı**

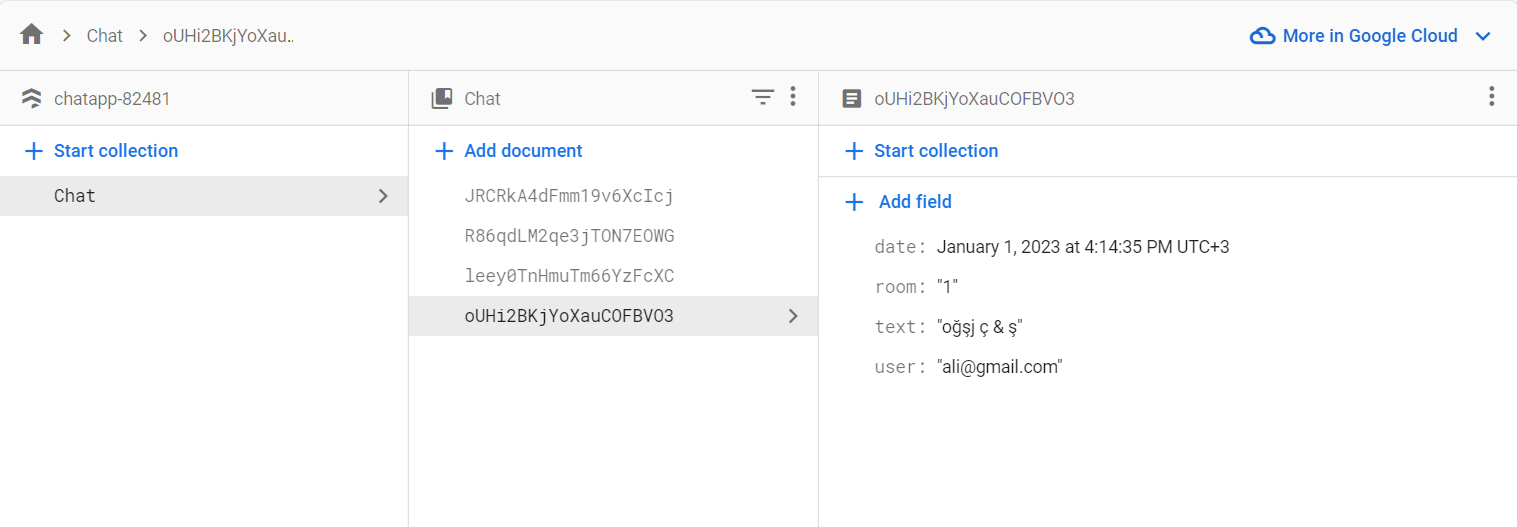
Odaya dahil olan kullanıcı, bu odada daha önceden yazılmış tüm mesajları ve kim tarafından yazıldıkları bilgilerini görebilir.



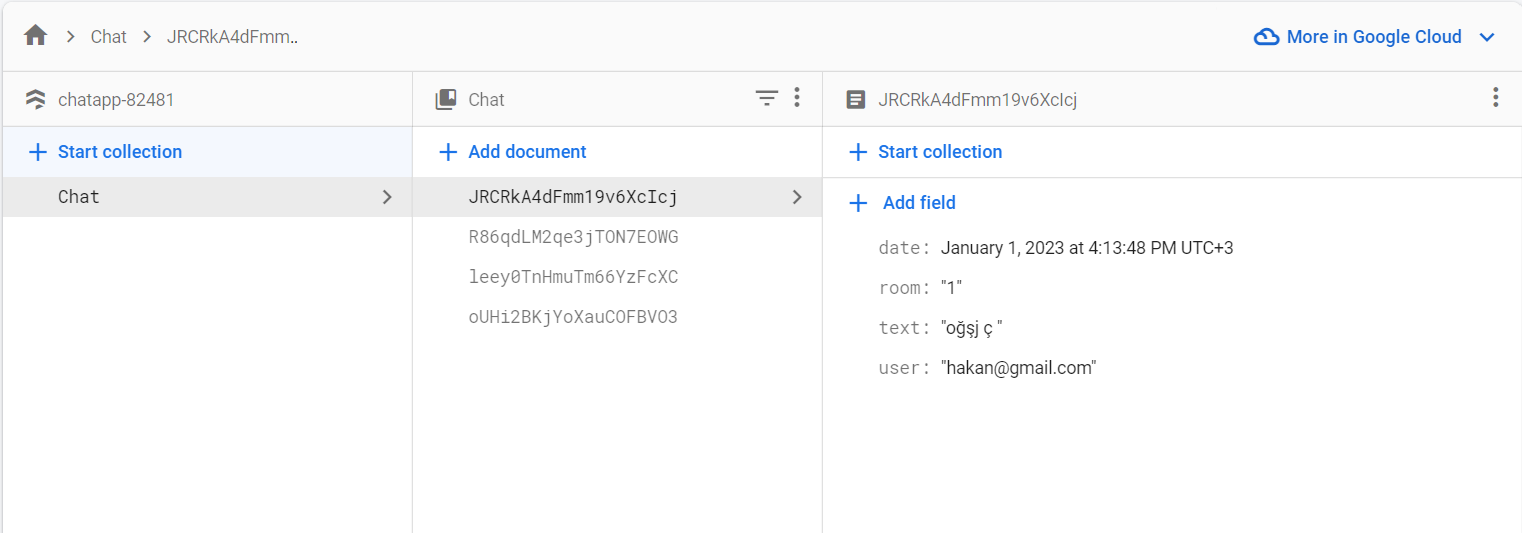
***Şekil 4.3.3.1***

**4.3.4.Mesajların Veritabanında Tutulması**

Girilen mesajlar şifrelenerek, kim tarafından yazıldıkları bilgisi , yazıldıkları oda numarası ve mesajın kaydedildiği tarih bilgileri ile veri tabanında kaydedilir.



***Şekil 4.3.4.1***

******

***Şekil 4.3.4.2***

**5.İlgili Çalışmalar**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Kaynak  Adı | Referans | Kapsam | Amaç | Kullanılan  Yöntemler | Sonuç |
| Vural, Hüseyin.  Trakya Üniversitesi Fen Bilimleri Enstitüsü,2014. | Trakya Üniversitesi Fen Bilimleri Enstitüsü | Simetrik şifreleme algoritmaların-  da blok şifrelerin anahtar genişletme algoritmaları. | *Simetrik şifreleme teknikle-*  *rinde anahtar planlama* | Literatürde bulunan AES ve ARIA blok şifrelerinin anahtar genişletme algoritmaları incelenmiş ve bu anahtar genişletme algoritmalarının incelenmesinden elde edilen tecrübe ile AES anahtar genişletme algoritmasına dayanan yeni bir anahtar genişletme algoritması geliştirilmiştir. | Geliştirilen yeni anahtar genişletme algoritması ve örnek test değerleri ile yeni anahtar genişletme algoritmasının çalışması gösterilmiştir. |
| Şahin, Fatih. "Modern blok şifreleme algoritmaları." *İstanbul Aydın Üniversitesi Dergisi* 7.26 (2015): 23-40. | *İstanbul Aydın Üniversitesi Dergisi* 7.26 (2015): 23-40. | Şifreleme; verinin, bilginin her şartta istenilen kişilere verinin güvenli bir şekilde iletilmesi için kullanılmaktadır. | Modern blok şifreleme algoritmaları- nın anlaşılması. | Simetrik ve Asimetrik şifreleme algoritmalarının yaygın kullanım yöntemleri. | Şifrelemede kullanılan anahtarın gücü ne kadarsa sistemin gücü de o kadardır. |
| YILMAZ, Menduh, and Serkan BALLI.  *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi* 2.2 (2016): 18-28. | *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi* 2.2 (2016): 18-28. | VERİ ŞİFRELEME ALGORİTMALARININ KULLANIMI İÇİN AKILLI BİR SEÇİM SİSTEMİ GELİŞTİRİLMESİ. | Bu çalışmada Akıllı Bir Seçim Sistemi geliştirilerek kullanıcıya anlık olarak, şifreleyeceği dosya türüne göre hangi algoritmayı seçmesi gerektiği konusunda yardımcı olmak amaçlanmıştır. | Şifrelemede simetrik ve asimetrik anahtarlı olmak üzere iki çeşit şifreleme türü kullanılmaktadır. | Bu çalışmada dosya türlerine göre belirlenen profiller doğrultusunda seçilen 6 tane şifreleme algoritmasının değerlendirilmesi yapılmıştır. |

**6.Sonuç**

Uygulama geliştirmeden önce amaçlanan, mesajların şifrelenmesi ve eski haline eksiksiz ve hatasız bir şekilde dönmesi sağlanmıştır. Kullanılan simetrik şifreleme algoritması, bir karakter kümesi kullanılarak, girilen metindeki her bir karakterin bu kümedeki karşılığını bulur ve 4 adım sonrasındaki karakter ile de-ğiştirir. Bu şifreleme algoritması karakter kümesi bir şekilde bilinen herkes tara- fından rahatlıkla çözülebilir. Kullanılan karakter kümesi soyutlanarak başka ki- şilerin görmemesi sağlanmalıdır.

Girilen mesajlar anlık olarak diğer kullanıcılar tarafından görüntülenebi- liyor.

**7.Kaynakça**

[1] Google, https://developer.android.com/guide/fragments, 2022-11-16

[2] Google, https://developer.android.com/develop/ui/views/layout/recyclerview,2022-12-22

[3] Google, https://firebase.google.com/docs/auth?authuser=1&hl=en, 2022-12-05

[4] Google, https://firebase.google.com/docs/firestore?authuser=1&hl=en, 2022-12-30